

Integration of Information Assurance (IA) into DoDAF Architectures

Annual Computer Security Applications Conference
(ACSAC '04)
8 December 2004

Edward Rodriguez
Booz Allen Hamilton

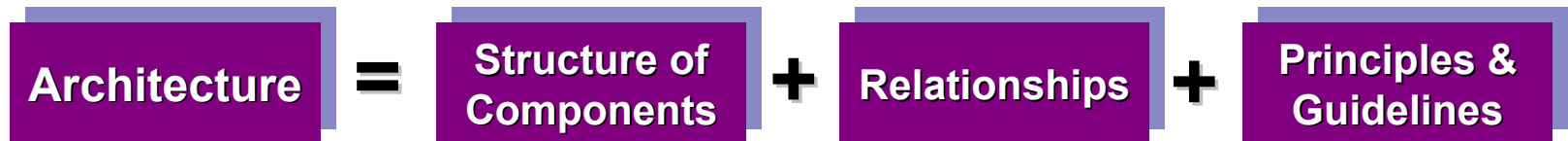
Agenda

- ▶ Enterprise Architecture Overview
- ▶ Problem Statement & Solution Approach
- ▶ Candidate Techniques to Integrate IA into DoDAF architectures
- ▶ Final Thoughts

Architecture Defined

"An architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution."

IEEE STD 1471-2000

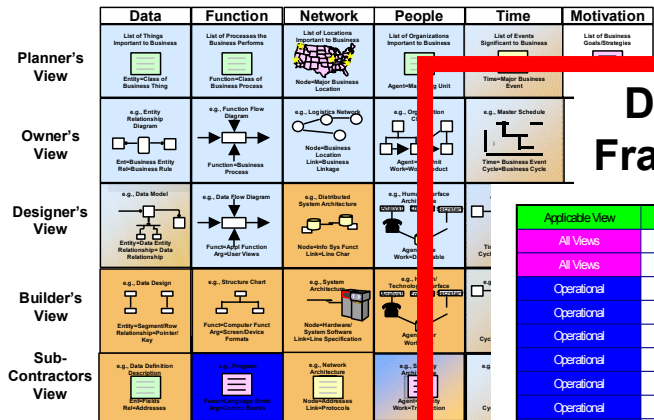


Purpose of the Enterprise Architecture

- ▶ *Inform*, *guide*, and *constrain* decisions for the enterprise
- ▶ Specifically:
 - Capture facts in an understandable way to promote better planning and decision making (IT investments)
 - Promote better communication (architectural views)
 - Improve consistency, accuracy, timeliness, integrity, quality of information
 - Achieve economies of scale, re-use, standardization, collaboration, shared services
 - Expedite integration of legacy, transition, target systems
 - Ensure legal and regulatory compliance

These Frameworks Are Focused on the Commercial, DoD/IC, and Federal Domains

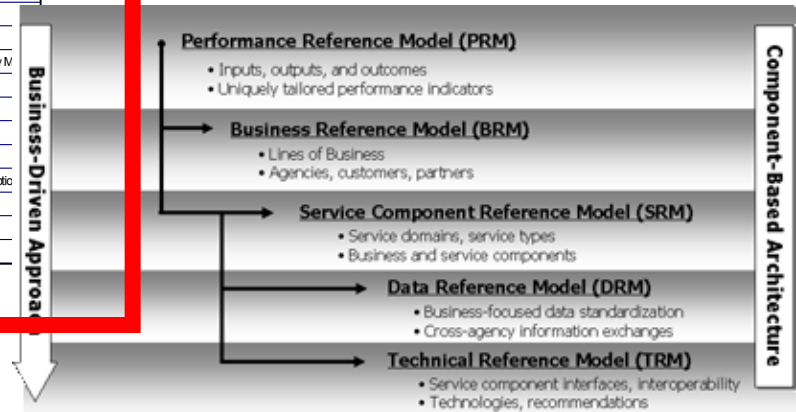
Zachman Framework



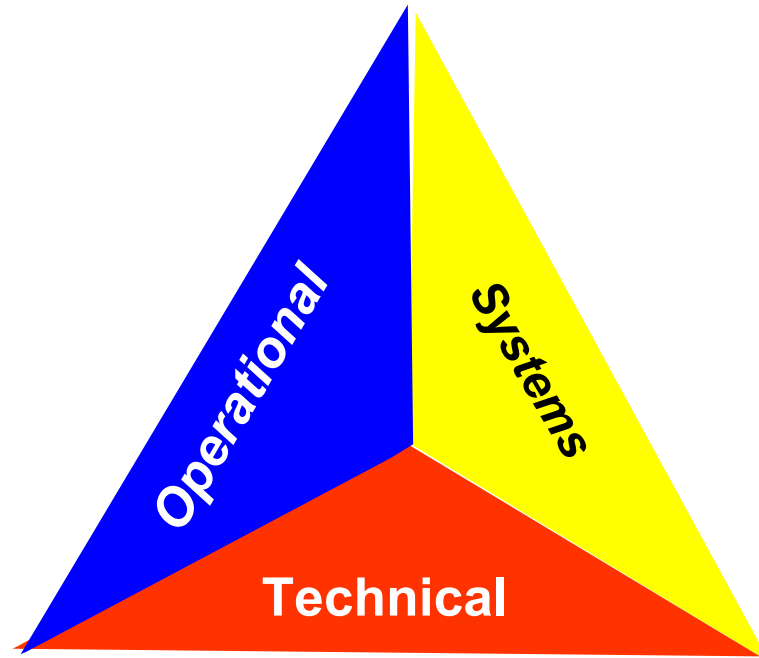
DoD Architecture Framework (DoDAF)

Applicable View	Framework Product	Framework Product Name
All Views	AV-1	Overview and Summary Information
All Views	AV-2	Integrated Dictionary
Operational	OV-1	High-Level Operational Concept Graphic
Operational	OV-2	Operational Node Connectivity Description
Operational	OV-3	Operational Information Exchange Matrix
Operational	OV-4	Organizational Relationships Chart
Operational	OV-5	Operational Activity Model
Operational	OV-6a, b, c	Operational Activity Sequence and Timing Descriptions
Operational	OV-7	Logical Data Model
Systems	SV-1	Systems Interface Description
Systems	SV-2	Systems Communications Description
Systems	SV-3	Systems-Systems Matrix
Systems	SV-4	Systems Functionality Description
Systems	SV-5	Operational Activity to Systems Function Traceability I
Systems	SV-6	Systems Data Exchange Matrix
Systems	SV-7	Systems Performance Parameters Matrix
Systems	SV-8	Systems Evolution Description
Systems	SV-9	Systems Technology Forecast
Systems	SV-10a, b, c	Systems Functionality Sequence and Timing Descriptio
Systems	SV-11	Physical Schema
Technical	TV-1	Technical Standards Profile
Technical	TV-2	Technical Standards Forecast

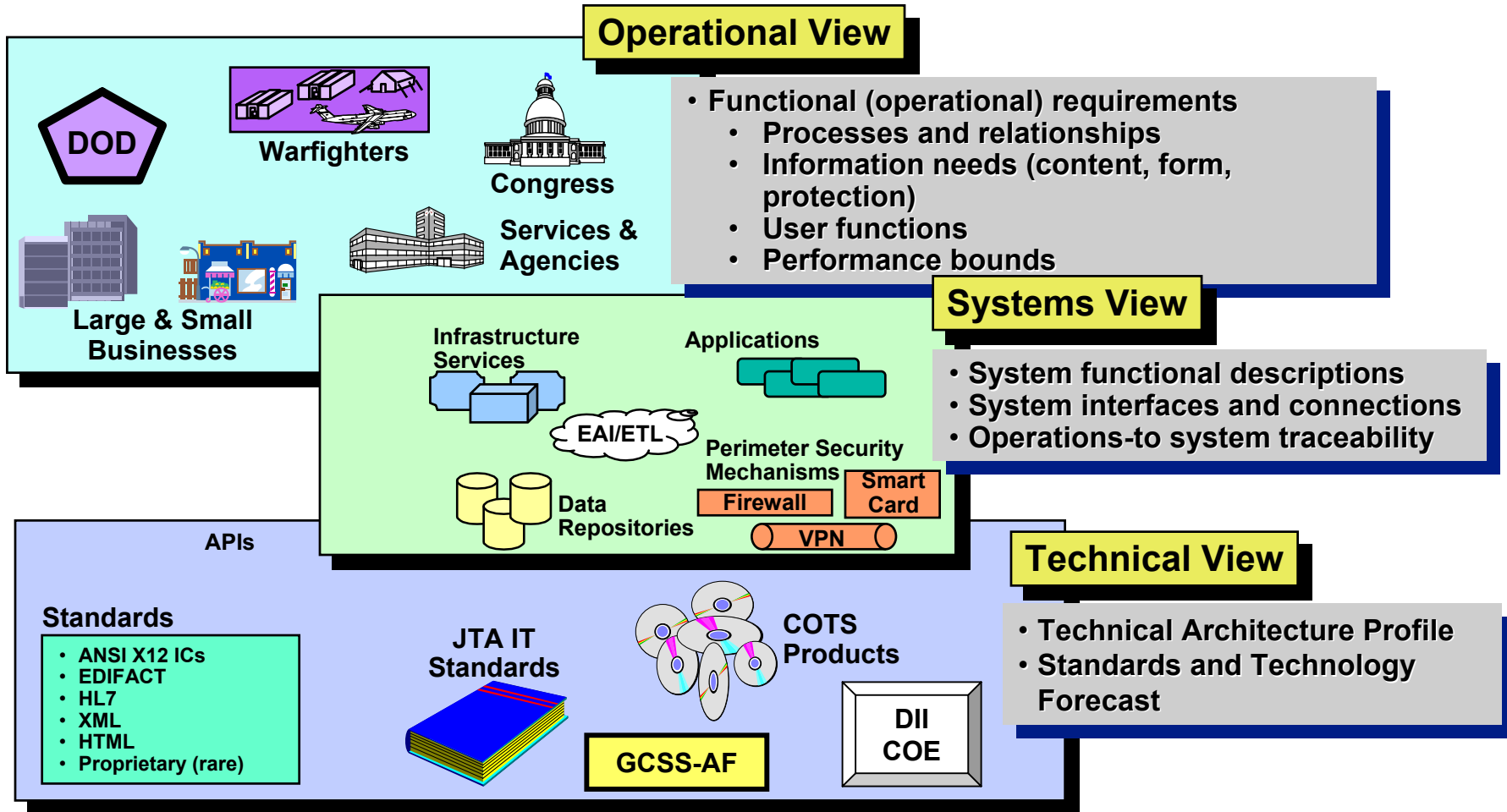
Federal Enterprise Architecture Framework (FEAF)



DoDAF Overview



DoDAF Architecture Views

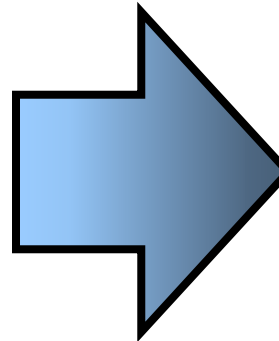


Problem Statement

DoD System Development Efforts Require Development Of DoDAF Architecture Early in the Life Cycle

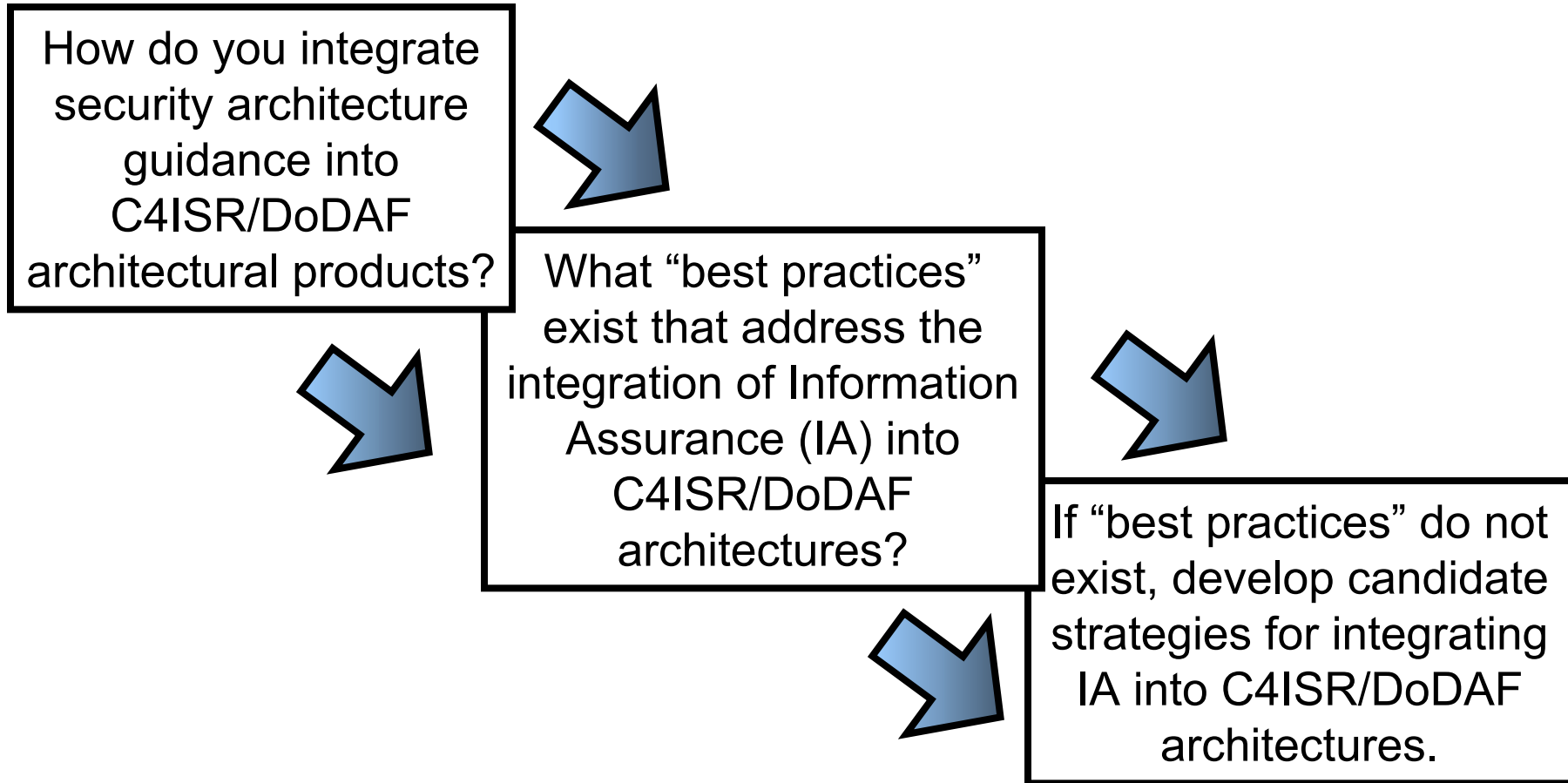
+

“Secure systems are developed most effectively by considering & integrating security early in the development life cycle”



How do you integrate security architecture guidance into C4ISR/DoDAF architectural products?

Approach to Solving Problem



Approach to Solving Problem

- ▶ Search for examples of efforts to integrate IA into C4ISR/DoDAF compliant architectures in public domain
- ▶ Search for guidance from DoDAF and C4ISR architecture government documentation
- ▶ Intra-company & community search for feedback on this topic
- ▶ Draw from personal exposure to assignments related to C4ISR/DoDAF products

Initial Findings

- ▶ Very limited information found via Web searches
 - In some instances “IA is important...” but that was all
- ▶ Search through DoDAF also yielded limited information/guidance
 - OV-2/3: Security/IA attributes included for needlines
 - TV-1: Inclusion of Security/IA standards
 - OV6b/c: Capture security activities & events

Initial Findings (cont.)

- ▶ One approach was to develop stand-alone narrative documents that describe the application of security services to the architecture and the identification of security oriented components
 - Not **integrated** into DoDAF framework
- ▶ Another employed approach was to identify some security services (SV-4), some limited OV-5 activities, and some security components (SV-1/2)
- ▶ One framework, TEF (Treasury Enterprise Architecture Framework), includes some security constructs

Not Much Found

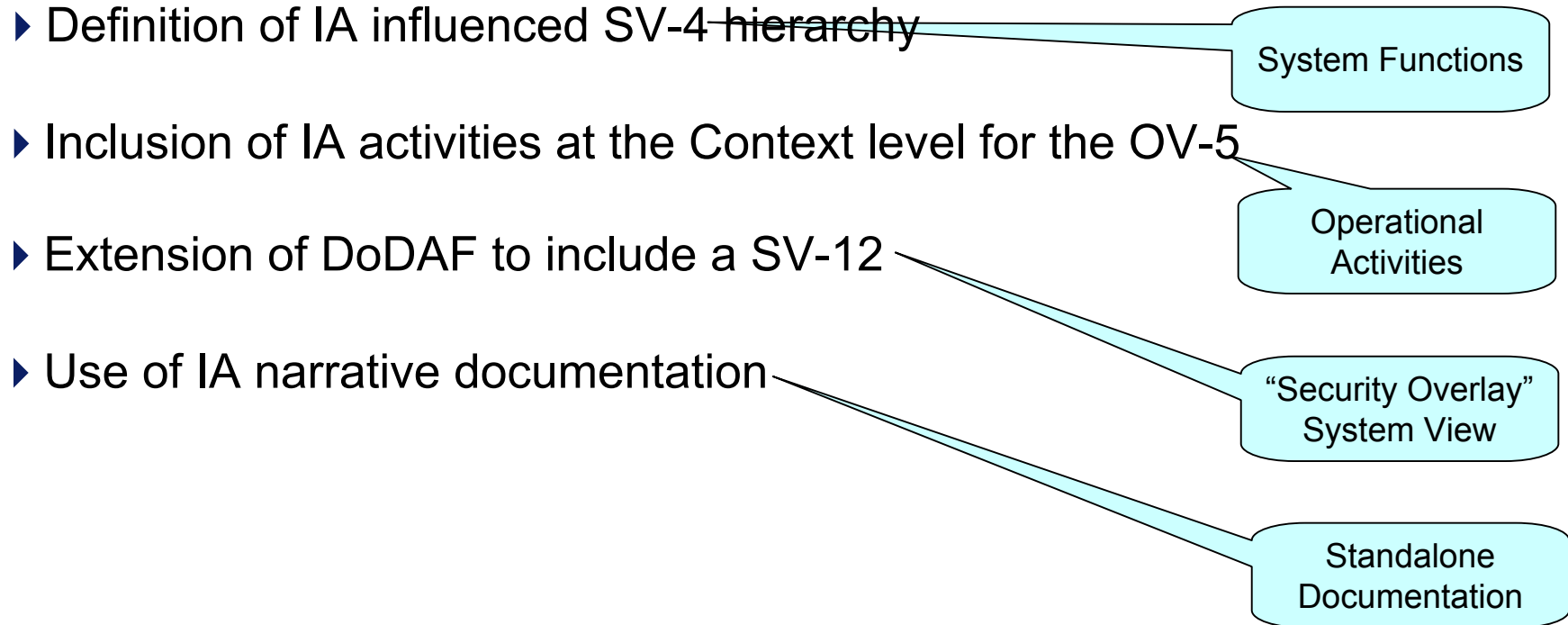
So the question remains...

Applicable View	Framework Product	Framework Product Name
All Views	AV-1	Overview and Summary Information
All Views	AV-2	Integrated Dictionary
Operational	OV-1	High-Level Operational Concept Graphic
Operational	OV-2	Operational Node Connectivity Description
Operational	OV-3	Operational Information Exchange Matrix
Operational	OV-4	Organizational Relationships Chart
Operational	OV-5	Operational Activity Model
Operational	OV-6a, b, c	Operational Activity Sequence and Timing Descriptions
Operational	OV-7	Logical Data Model
Systems	SV-1	System Interface Description
Systems	SV-2	Systems Interconnectivity Description
Systems	SV-3	Systems Security Matrix
Systems	SV-4	Systems Functionality Description
Systems	SV-5	Operational Activity to Systems Function Traceability Matrix
Systems	SV-6	Systems Data Exchange Matrix
Systems	SV-7	Systems Performance Parameters Matrix
Systems	SV-8	Systems Evolution Description
Systems	SV-9	Systems Technology Forecast
Systems	SV-10a, b, c	Systems Functionality Sequence and Timing Descriptions
Systems	SV-11	Physical Schema
Technical	TV-1	Technical Standards Profile
Technical	TV-2	Technical Standards Forecast

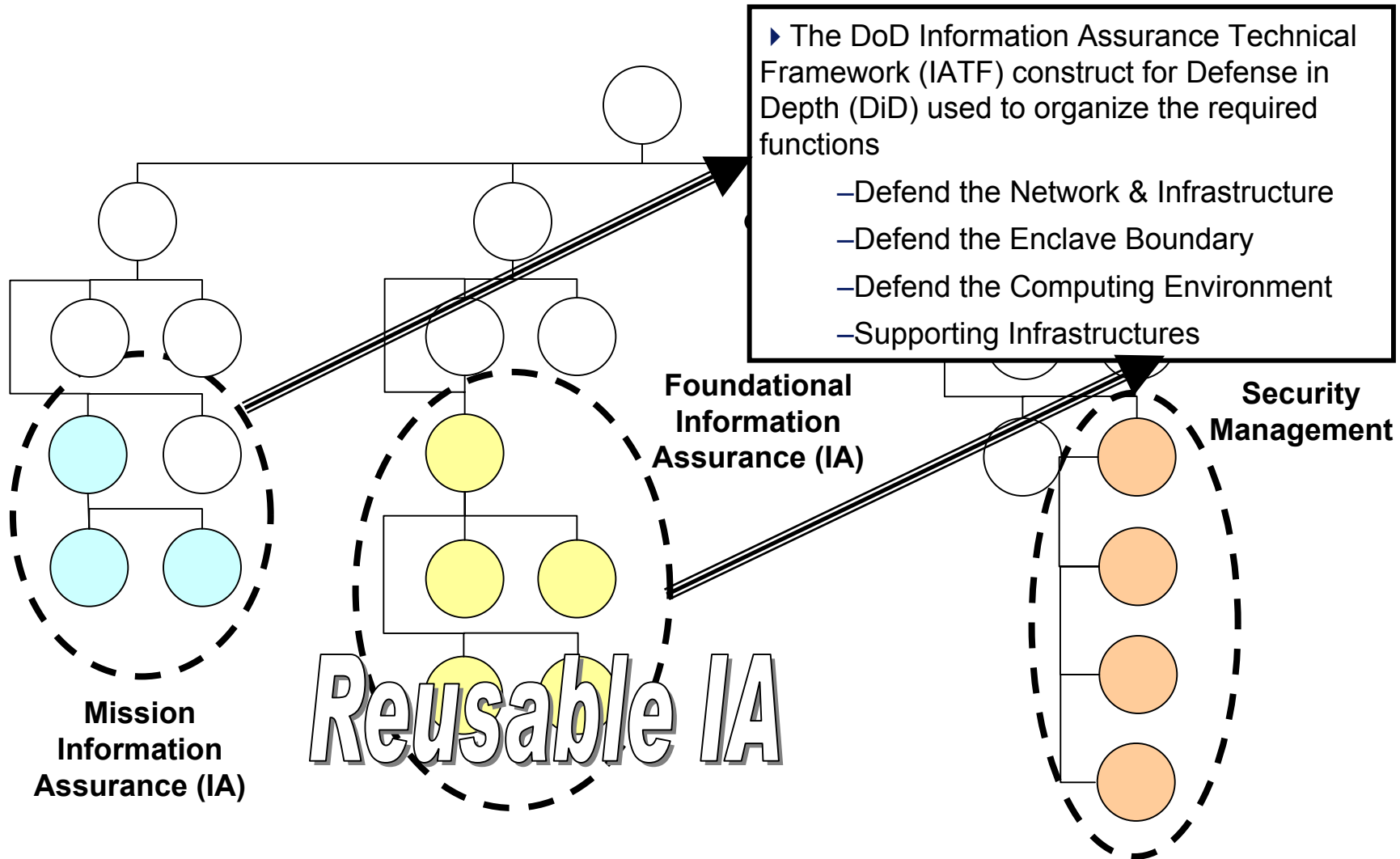
C4ISR/DoDAF

+ IA = ?

Proposed Practices for IA Integration into C4ISR/DoDAF Architectures

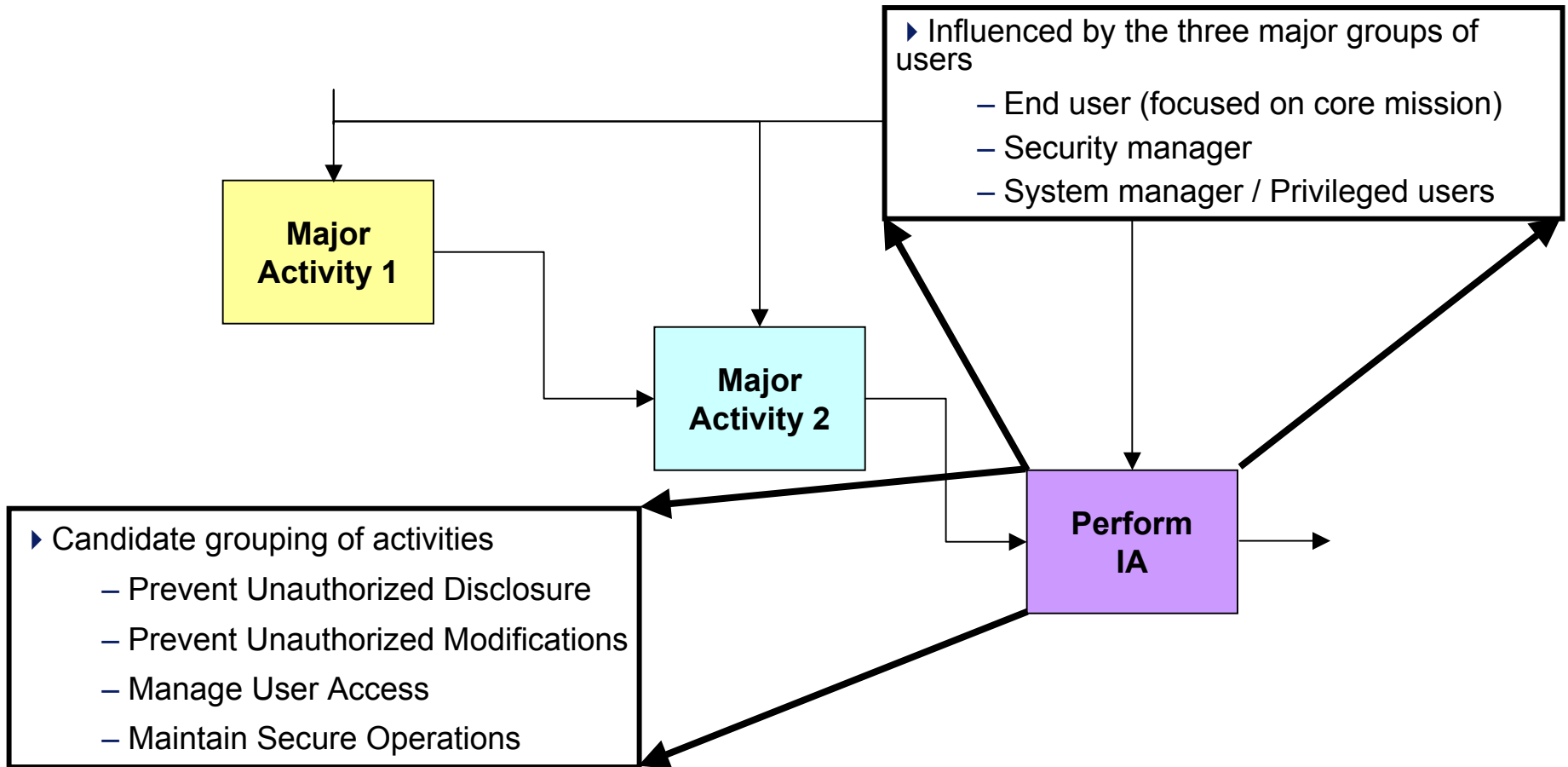


IA Influenced SV-4 Hierarchy



IA Influenced OV-5 Construct

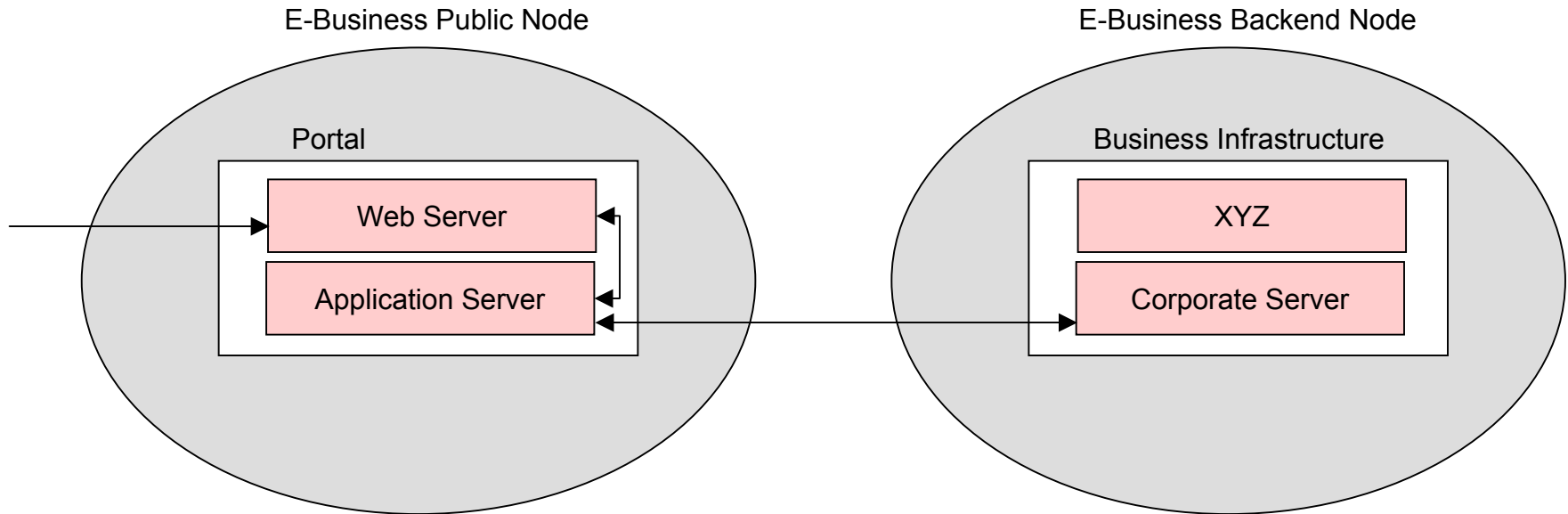
► Inclusion of IA activities at the Context level



Extension of DoDAF to include a SV-12

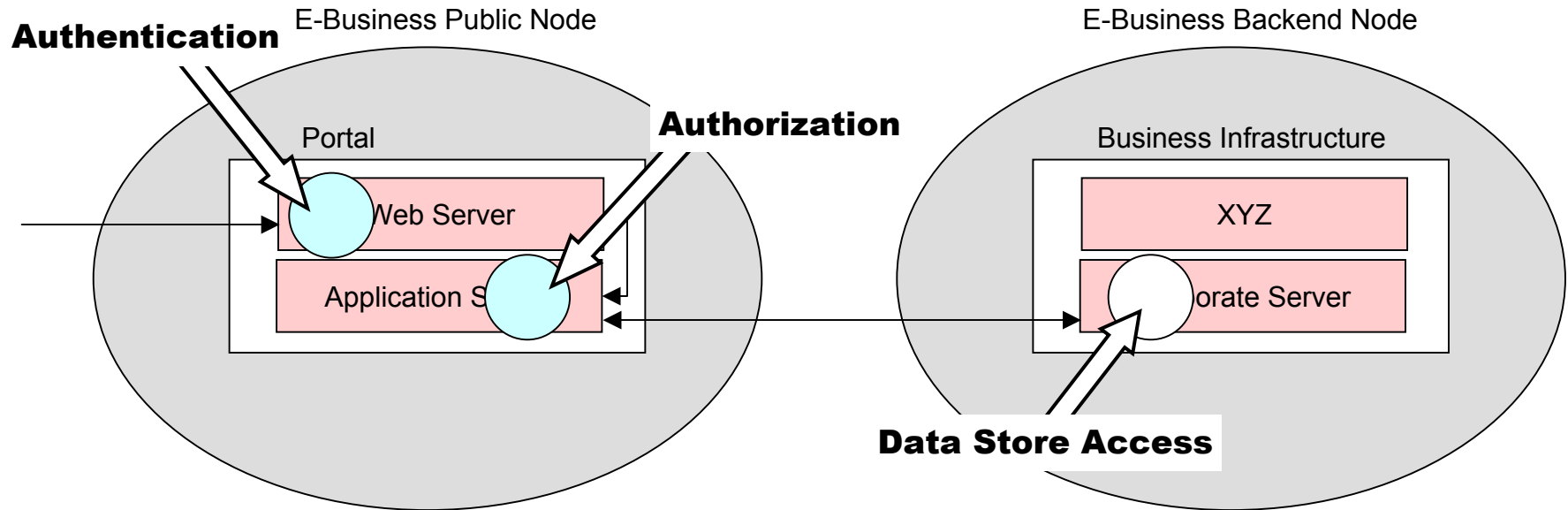
- ▶ DoDAF allows the definition of additional views
- ▶ SV-12, Security Overlay, is a supplemental view focused on IA specific characteristics of the system
 - Uses only data elements currently defined by existing System Views
 - Allow a security oriented view consistent with the rest of the DoDAF architecture
- ▶ Initially performed via “Powerpoint™ Engineering”
 - Not an **integrated** architecture approach
 - Therefore, arguably, not in compliance with DoD direction/guidance regarding the development of “integrated architectures”

Notional SV-12 – User Login



SV-1 View provides a perspective associated with the physical dimension of the system

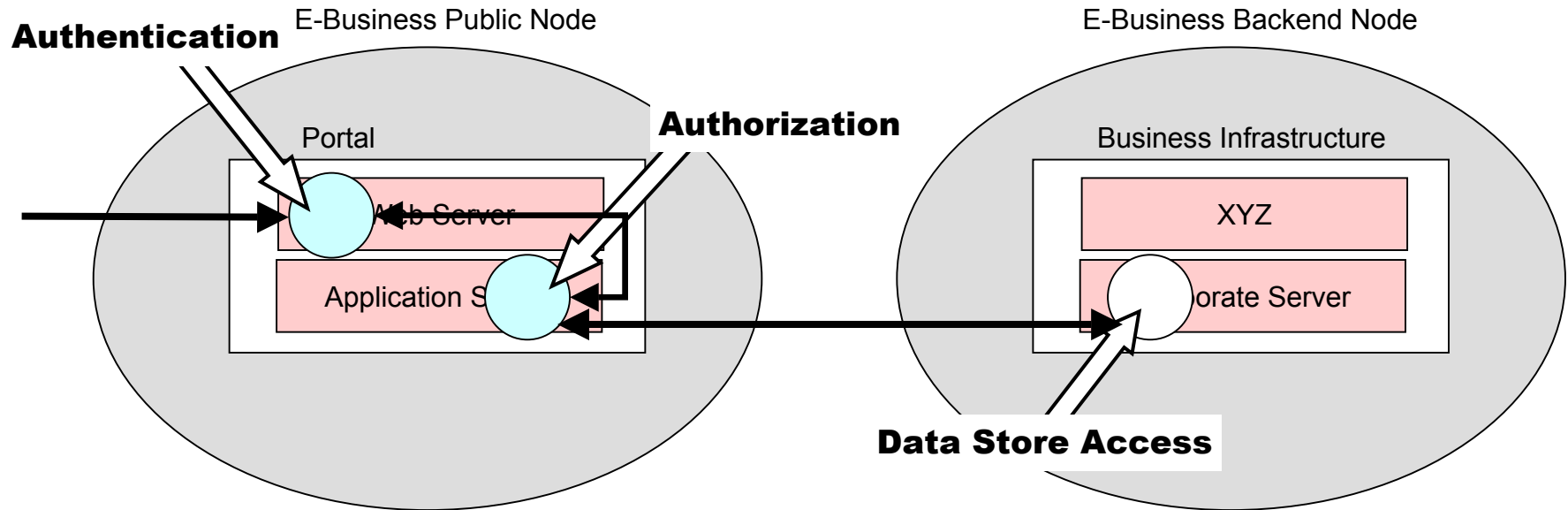
Notional SV-12 – User Login



SV-4 functions used to accomplish a particular security related activity are overlay on the system elements where the functions are executed

For some security functionality, it matters where the function is performed

Notional SV-12 – User Login



SV-4 data flows specifically used by the selected functions to accomplish the particular security related activity are added

***Where functions are fairly complex, it is important to define specific data flows
Note: sequencing information not included... Separate SV-10c diagram required***

SV-12 Usage

- ▶ Useful to create views for the various topics that Certification and Accreditation (C&A) staff require information and knowledge on
 - Authentication
 - Login for General Users
 - Login for Privileged Users
 - System auditing
 - Etc.
- ▶ Powerful to discuss these topics with artifacts that are consistent and **integrated** with the overall architecture and underlying data models
 - Also helps to explain how the security requirements are to be met
- ▶ Refinement of SV-12 concept likely as feedback from various stakeholders is received and lessons learned applied

Use of IA Narrative Documentation

- ▶ Narrative documentation may still be required for those stakeholders that are uncomfortable with C4ISR/DoDAF views
- ▶ May be required to support C&A documentation requirements
 - Nonetheless, opportunity to couple Security documents (e.g., Security CONOPS) to key C4ISR artifacts

Final Thoughts

Why hasn't Security Been More Integrated Into Enterprise Architecture Frameworks?

- ▶ Historically, security awareness has lagged behind emphasis on functionality and performance
- ▶ The importance / business value of security is not easily quantifiable
 - How do you calculate ROI?
- ▶ Other possible hypotheses
 - Limited input by the security community in regards to **what is important** to capture from an architectural perspective
 - Limited input by the security community in regards to **how to capture** what is important within the existing architectural frameworks

Final Thoughts

- ▶ Just a few steps to hopefully move DoDAF community in a constructive direction in the area of integrating IA into C4ISR/DoDAF architectures
- ▶ If security knowledgeable professionals don't actively seek out opportunities to integrate the IA dimension into main stream system engineering processes then it won't naturally happen
- ▶ These ideas are not the product of any one individual, so thanks and acknowledgements are due:
 - Tom Vander Vlis
 - Barry Lewis
 - Frank Kroll

Thanks

Ed Rodriguez
Senior Associate

Booz | Allen | Hamilton

Tel (301) 543-4660
rodriguez_ed@bah.com

Booz | Allen | Hamilton

delivering results that endure

Booz | Allen | Hamilton